**For the:** University of Strathclyde Students’ Association

**Last updated:** 4th April 2023

**Approved by:**

# Introduction

The University of Strathclyde Students’ Association (also referred to as “Strath Union”) is a charitable organisation whose registered address is 90 John Centre, Glasgow, G1 1JH. The Students’ Association has approximately employs staff and volunteers based from the above premises.

The charitable purposes of the Students’ Association, as stated on the [website of the Scottish Charity Regulator](https://www.oscr.org.uk/about-charities/search-the-register/charity-details?number=SC005914), are:

*“…the advancement of education of Students at The University of Strathclyde for the public benefit by: … promoting the interests and welfare of Students at the University of Strathclyde during their course of study and representing, supporting and advising Students; … being the recognized representative channel between Students and the University of Strathclyde and any other external bodies; … providing social, cultural, sporting and recreational activities and forums for discussions and debate for the personal development of its Students.”*

# Policy Statement

1. The Students’ Association intends to comply with the relevant data protection legislation in the UK at the time of writing, including:
	1. The UK General Data Protection Regulation (UK GDPR)
	2. The Data Protection Act 2018
	3. The Privacy and Electronic Communications Regulations
2. We will therefore abide by the data protection principles set out in Article 5 of UK GDPR:
	1. *‘lawfulness, fairness and transparency*’: We will process personal data fairly and transparently, and only ever on one of the lawful bases outlined in UK GDPR Article 6
	2. ‘*purpose limitation’*: We will only process personal data for specific purposes, relating to the charitable objectives of the Students’ Association
	3. *‘data minimisation’:* We will only process as much personal data as is necessary for our administration and the services we supply.
	4. ‘*accuracy*’: We will keep the personal data we process accurate, and where necessary up-to-date. In particular we will strive to rectify data when made aware of any inaccuracies.
	5. ‘*storage limitation’*: We will only process personal data for so long as necessary for the Association’s charitable purposes. We have determined that a period of seven years following the last contact with an individual is an appropriate maximum period to hold data covering the legal limitation period for certain financial purposes (covering six years after the tax year in which a transaction occurs) .We will process and store other non-financial data for shorter time periods as appropriate.
	6. ‘integrity and confidentiality’: We will take appropriate organisational and technical measures to ensure that Personal Data processed by us is kept secure. Where we use third party data processors, we will choose them carefully with a view to their data security and compliance with GDPR and have GDPR compliant contracts with them.
3. We will also seek to ensure that individual data subjects’ rights are respected. In particular:
	1. We will send or otherwise provide appropriate notices (according to UK GDPR Articles 13 and 14) to those whose personal data is processed by us including our employees, volunteers and individuals or individuals within partners who supply us with goods or services. We will also make such notices available to individuals to whom we send generic marketing communications (e.g. newsletters).
	2. We will not engage in direct marketing to clients or prospects otherwise than in accordance with the relevant legislation and guidance from the ICO.
	3. We will respond to any individual data subject exercising their rights under UK GDPR, in particular the rights to:
		* Access;
		* Rectification;
		* Erasure;
		* Restriction of processing;
		* Objection to processing
	4. Our policy is not to charge a fee to data subjects for exercising any of the above rights, but we may decide not to act on the request if it is “manifestly unfounded or excessive” according to UK GDPR article 12(5)
4. The Students’ Association is not obliged to formally appoint a Data Protection Officer under UK GDPR, as we do not believe any of the conditions in article 37(1) apply. <role> is, however, appointed as our Data Protection Lead.
5. The Students’ Association will not transfer Personal Data (which includes giving third parties access to it within our IT system) to recipients located outside the European Economic Area and the UK without confirmation from our Data Protection Officer that such transfer is lawful.

# University of Strathclyde Students’ Association’s Status as Data Controller

The Students’ Association is a data controller, as it determines the purposes and the means of processing personal data, in the course of pursuing its charitable objectives.

We have determined that we are joint controllers with the University of Strathclyde with respect to the data shared to manage our members, course representatives and those identified within meeting minutes. We have a data sharing agreement in place with the University of Strathclyde which sets out in more detail the relationship between the two organisations as joint controllers.

Additionally, we engage data processors to act on our behalf. These data processors are listed later in this document.

We have determined that when employee, trustee or members data is shared by the Students’ Association with our pension provider, insurance provider, HMRC, BUCS and National Governing Bodies, these bodies are data controllers in their own right as they decide their own purposes and means of processing once the personal data is shared. We will, where possible, require agreements with them containing confidentiality obligations in respect of that data and other data that they create relating to our employees, members or customers in the context of the work they are doing.

# Description of Data Processing (including special category data)

**Full, associate and affiliate members**

|  |  |
| --- | --- |
| **Personal data collected:** | Student ID, Email Address, Full Name, Gender, Faculty, Department, Course, Year of Study, Level of Study, Mature Student, PT or FT Status, DL Status, Domicile, Graduation Year, Fee Paying Status, Parent/Carer, Telephone, Images of the Individual, Postal Address, Group Membership, Date of Birth, Age, NI Number, DVLA Number, Signature, Next of Kin Details and Course Instance Location |
| **Special categories of data collected:** | Ethnicity |
| **Data origination:** | University of Strathclyde, directly provided by the student |
| **Storage location:** | i-Drive, Club Management Portal, Website Server, Qualtrics, Xero and Stripe. |
| **Identified data usage:** | Membership records, advice centre user records, CCTV meeting minutes, records of attendance at events, event attendance, purchase history, elections & referenda voting history, democratic engagement history, registered driver details, newsletter subscriptions, inbound and outbound payments, refunds, retail purchase history, group membership, course rep records, research engagement, have your say idea engagement, health and safety records, medical records and sports club registration history |

|  |  |
| --- | --- |
| **Third parties with access:** | University of Strathclyde, National Governing Bodies, BUCS, SSS and Endsleigh |
| **Retention period:** | 7 years |

**Customers and visitors**

|  |  |
| --- | --- |
| **Personal data collected:** | Image of individual, Postal Address, Telephone, Email Address, Full Name and Student ID |
| **Special categories of data collected:** | None |
| **Data origination:** | Provided by individual |
| **Storage location:** | CCTV Control Units (Offline), Xero, PayPal and Stripe. |
| **Identified data usage:** | CCTV, Event ticket sales history, inbound and outbound payments, refunds and retail purchase history |
| **Third parties with access:** | None |
| **Retention period:** | Maximum of 7 years in the case of financial transactions. |

**Employees of suppliers, contractors and clients**

|  |  |
| --- | --- |
| **Personal data collected:** | Email Address, Full Name, Business Name, Postal Address, Role Title, Telephone, Signature and Bank Details |
| **Special categories of data collected:** | None |
| **Data origination:** | Provided by individual |
| **Storage location:** | Xero, Locked Filing Cabinet and i-Suite |
| **Identified data usage:** | Client invoices, supplier payments, marketing and communications, credit management and fraud prevention |
| **Third parties with access:** | Auditors, Financial Advisor and Media Agency |
| **Retention period:** | Maximum of 7 years in the case of financial transactions. |

**Employees of the Students’ Association**

|  |  |
| --- | --- |
| **Personal data collected:** | Email Address, Full Name, Telephone, Postal Address, Role Title, Date of Birth, Gender, NI Number, Bank Details, P45 / P46, Next of Kin Details, Disciplinary Record, Financial Bonding, Photographic ID, Business Interests, Family Relationships, Right to work in UK, Reference Personal Details, Course, Year of Study and Student ID |
| **Data origination:** | Provided by individual |
| **Special categories of data collected:** | Criminal Record and Personal Health Records |
| **Storage location:** | Locked Cabinet, Santander Bank, G-Suite, i-Drive, BreatheHR and Xero |
| **Identified data usage:** | Employee Administration, Recruitment processes and Expense claims |
| **Third parties with access:** | Students’ Association solicitors and National Health Service |
| **Retention period:** | Recruitment records - 6 weeks after not being appointed to a role HR records – maximum 7 years after the employment ends. |

# Our Lawful Bases for Processing Personal Data (including conditions relied on for processing special category data)

The different lawful bases we rely on to process personal data lawfully are listed below, with details of when they are relied upon, and in regard to what personal data:

# Consent

We are aware that consent under UK GDPR must be freely given, specific, informed and unambiguous given by a statement or a clear affirmative action and that we have to keep a record of each consent obtained for as long as we are using it. We do not currently believe that any of our processing of Personal Data requires data subject consent, except for the below-mentioned political campaigning and related activities,

As our members have purchased through their tuition fees a membership of the Students’ Association, we do not need consent in communicating through digital means with our members about our related charitable products and services. We believe that we have a legitimate interest in providing this information according to UK GDPR article 6(f). In all communications there is an opt-out and the member will have received privacy information before receiving any communications at all.

Where the Students’ Association uses personal data while undertaking campaigning, lobbying, communicating a political standpoint or acting as a conduit for commercial marketing activities (undertaken by our subsidiary trading company on behalf of third-party clients) explicit consent shall be obtained. In this way we will ensure that the special category data (in this case, political opinions) is lawfully processed according to UK GDPR article 9(2)(a).

The Students’ Association follows industry guidance relating to research gathering. Where personal data is collected as part of a research exercise, for ethical reasons this shall be undertaken by asking individuals for their consent to proceed. However, because of the nature of research, we will not rely on consent as a lawful basis for processing under GDPR. Instead, we will rely on our legitimate interest (article 6(1)(f)

# Compliance with a legal obligation

Together with the University of Strathclyde we have interpreted The Education Act to require all University of Strathclyde students to be members unless they opt-out, which revokes any requirements to receive explicit consent for data processing in relation to the administration of membership. We are required to deliver certain services by the Education Act for our members, and hence we rely on this lawful basis for the initial collection and processing of student personal data once they have enrolled on a University course..

# Performance of a contract to which the data subject is party

When individuals purchase products or utilise services through our trading company we have access to process this data to administer our contracted duties.

# Legitimate Interests

We rely on legitimate interest to justify much of our processing of Personal Data as we have assessed that the majority of our processing activity would be in the reasonable expectations of those we process data about. Our activities reliant on legitimate interest are as follows:

# *Employees:*

We require the data processing to enable us to be a good employer and pay employees. Whilst they are candidates we require it to assess them for employment. Employees and candidates expect us to hold and process that personal data for those purposes. We destroy candidate personal data if the candidate is unsuccessful.

Once employed, many aspects of the data processing performed as part of the employee’s relationship with the Students’ Association as employer will be covered directly by an employment contract. However, many aspects will not be explicitly covered in the employment contract, and so we rely on our legitimate interests to process personal data for all employees.

# *Members:*

As a membership organisation processing individual data is central to our service provision. Members are able to opt-out of processing by terminating their membership. To provide a high standard of service and personalise our provision we record and process data relating to members engagement and communications preferences. The maximum study term for a student is 7 years and we retain student data for a further 3 years to a maximum of 7 years. Our data is refreshed annually by the University.

We are satisfied that our activities are in our legitimate interest as we provide products and services to our members and that these activities do not risk the rights and freedoms of the individuals concerned. Our members are informed of our processing activities an Article 14 notice served at enrolment.

# *Suppliers, partners and clients:*

Our suppliers, partners and customers are not usually individuals so here we are dealing with the identifiable employees of our suppliers and clients who require us to deal with such individuals or self-employed individuals. We require their personal data (email, office address, and telephone numbers) to enable us to contact them in the context of their job. If an employee leaves a client or supplier we remove their details from the CRM and other systems (or we would be communicating with the wrong person). They expect that we will hold their contact details for this purpose. We therefore rely on our legitimate interests as a basis for processing this data.

In all the above cases we believe that we have a legitimate interest in carrying out that processing and that the processing has no significant risk to the rights and freedoms of the individuals concerned.

# Data Processors

We have identified the following parties as “data processors” (as defined in article 4(8) of UK GDPR):

* University of Strathclyde - In the provision of managed servers (I and K Drives)
* Google - In the provision of G-Suite applications
* GoDaddy - In the provision of Students’ Association website servers
* CRC Software Solutions - In the provision of Students’ Association website servers
* Microsoft - In the provision of an intranet service (using Sharepoint)
* Xero - In the provision of accounting software
* Qualtrics - In the provision of research tools

# The above parties either have a direct contract using the Students’ Association model contract or through GDPR compliant terms and conditions of use of service.

All our data processors undertake to keep the data within the EEA or put in place appropriate safeguards to protect the transfer of personal data outside the EEA, in accordance with UK GDPR.

# Organisational and technical measures

We use the following organisational and technical measures to ensure the confidentiality of personal data:

* Our physical premises are locked and alarmed when not occupied.
* Employees and volunteers who process data are required to consider the use of lockable filing cabinets, secure storage for archived files and the use of a shredder or confidential waste bin for hard copies of paperwork, file notes, incoming and outgoing letter correspondence containing personal data.
* For electronically held data, employees and volunteers who process data are required to consider
	+ using storage on the University network, work i-suite or platforms approved by the Data Protection Officer;
	+ password protection on all files containing personal data;
	+ the use ofthe Students’ Association secure platforms for processing data;
	+ Keeping software up-to-date by installing updates without undue delay;
	+ running up to date antivirus and antimalware software;
	+ installation of adequate firewalls,
	+ secure disposal of IT equipment.
* CCTV units are not networked and access to the systems is gained through password protected platforms.
* Email accounts are individually assigned and by policy are not to be shared with colleagues or third parties. Access to emails is only authorised for third parties for specific purposes by Senior Management Team members.
* The data protection and information security handbook provides clear guidance on data sharing, data handling, security breach procedures and disposal of data.
* We hold GDPR compliant contracts with all data processors.
* All employees and volunteers undertake training in data privacy law and cyber security before being given authorised access to process data held by the Students’ Association.

# Privacy Information provided to data subjects

In line with articles 13 & 14 of UK GDPR, we will send or otherwise provide appropriate notices to those whose personal data is processed by us including our employees, volunteers and individuals or individuals within partners who supply us with goods or services. We will also make such notices available to individuals to whom we send generic marketing communications (e.g. newsletters).

We provide 4 privacy statements via the Strath Union website ( https://www.strathunion.com/union/governance/dataprotection/ ) aimed at 4 different audiences:

* Student: (https://www.strathunion.com/union/governance/dataprotection/studentdataprivacy/ ):
* Employee: (https://www.strathunion.com/union/governance/dataprotection/employeeprivacystatement/ )
* Supplier: (https://www.strathunion.com/union/governance/dataprotection/supplierprivacynotice/ ):
* Consumer: (https://www.strathunion.com/union/governance/dataprotection/consumerdataprivacynotice/

We do not believe that articles 13 & 14 require notice to be sent to every data subject whose personal data we are processing. Following advice we have concluded that employees of our current or prospective partners and suppliers whose contact details we need to use for dealing with those organisations, and individuals who simply engage in correspondence with us, do not need to have privacy information pro-actively provided (as the effect of interpreting UK GDPR otherwise would be disproportionate.)

# Individuals’ Rights – responding to requests from data subjects

UK GDPR sets out various rights that data subjects have, namely the rights to:

* *be informed:*
* *access personal data;*
* *request rectification;*
* *request erasure;*
* *request restriction of processing*
* *object to processing*
* *object to automated decision making*
* *data portability*

The right to be informed is satisfied via Strath Union’s privacy statements, as mentioned above.

The Students Association will ensure that any personal data can be made available or transferred using a “commonly used and machine-readable format” according to UK GDPR article 20.

Any objection to automated decision making will be responded to by stating the fact that the Students’ Association does not engage in any purely automated decision making with either legal or similarly significant consequences.

For all other data subject rights requests, the Students’ Association will act according to the requirements in UK GDPR, namely by responding within one calendar month, with the possibility of extending the deadline for response by 2 further months if necessary.

We may suggest that data subjects use our Data Subject Rights Request Form to submit their requests. However, we will not require this form to be used, as UK GDPR specifies that requests can be made via any medium and without using any particular form of words,

The Students’ Association will not charge a fee to data subjects for exercising any of the above rights but may decide not to act on the request if it is “manifestly unfounded or excessive” according to UK GDPR article 12(5). The Students’ Association will also need to satisfy itself of the identity of the requester, and so may ask the requester to provide proof of identity.

Any employees or volunteers acting on behalf of the Students’ Association should refer any such rights request to the Data Protection Lead without undue delay, regardless of the manner in which the request is made.